REMARKS

Claims 1-12 and 14-18 are pending. Claims 1, 7, and 12 are in independent form.

Independent Claim 1

In the action mailed August 24, 2005, claim 1 was rejected under 35 U.S.C. § 103(a) as obvious over U.S. Patent No. 6,073,165 to Narasimhan at al. (hereinafter "Narasimhan") and U.S. Patent No. 6,704,768 to Zombek et al. (hereinafter "Zombek").

Claim 1 relates to a method that includes obtaining, at a first node, information indicative of a network condition, encapsulating said information into an HTTP protocol, and sending said HTTP protocol to a network managing node.

The rejection of claim 1 contends that Zombek describes the HTTP encapsulation of SNMP messages. In support of this contention, the rejection points to col. 13, line 15-32.

Applicant respectfully disagrees. Zombek describes that his network servers support *standard* SNMP operations. *See Zombek*, col. 13, line 16-17. One of Zombek's servers, namely server SNMP console 130, provides network management services. *See Zombek*, col. 11, line 24-29. These services are provided to all of Zombek's intelligent messaging network servers. *See Zombek*, col. 11, line 20-23. These network servers include PG

116, MR 124, HTTP Proxy Back End Server 132, and BES 122. *See Zombek*, col. 13, line 24-29. Registrations with SNMP console 130 can be encapsulated by a set of application programming interfaces API's provided by server SDK. *See Zombek*, col. 13, line 29-32.

Applicant submits that the mere provision of standard SNMP services by SNMP console 130 neither describes nor suggests the HTTP encapsulation of SNMP messages. There is simply no basis to believe that Zombek's SNMP messages are HTTP encapsulated. Moreover, the mere fact that SNMP console 130 provides standard SNMP services to an HTTP Proxy Back End Server 132 does not mean that messages for these standard SNMP services are HTTP encapsulated. As Zombek points out, SNMP is the standard protocol used in conventional TCP/IP networks. *See Zombek*, col. 11, line 29-31. Further, all of Zombek's servers provide "server-to-server TCP/IP communication" services. *See Zombek*, col. 12, line 66- col. 13, line 8. Conventional SNMP communication thus appears to be available to SNMP console 130, whether communicating with HTTP Proxy Back End Server 132 or with another of Zombek's servers. Since communication over a conventional TCP/IP network need not be HTTP encapsulated, there is no reason to believe that the standard services provided by SNMP console 130 are HTTP encapsulated.

Further, there is simply no indication that the API's provided by server SDK encapsulate registrations with SNMP console 130 into an HTTP protocol. The mere fact that some encapsulation occurs does not necessarily require HTTP encapsulation. As Zombek points out, the API's provided by server SDK can support the various network-supported platforms and networks. *See Zombek*, col. 12, line 40-42. Many of these networks require their own flavor of encapsulation. *See Zombek*, col. 18, line 49-54. Thus, non-HTTP encapsulation both exists and is present in Zombek.

In summary, nowhere does Zombek describe or suggest encapsulating information indicative of a network condition into an HTTP protocol, as recited in claim 1.

Narasimhan adds nothing to remedy this deficiency in Zombek. As discussed in the response filed June 10, 2005, Narasimhan presents SNMP and HTTP as separate protocols. Nowhere is there any teaching or suggestion that information indicative of the network condition is encapsulated in HTTP. Rather, the information about the network condition is apparently sent as SNMP, as conventional, and there is a separate communication via HTTP.

Since elements and/or limitations of claim 1 are neither described nor suggested by the cited art, a *prima facie* case of obviousness has not been established. Accordingly, applicant

requests that claim 1, and the claims dependent therefrom, be allowed.

Independent Claim 7

Claim 7 was rejected under 35 U.S.C. § 103(a) as obvious over U.S. Patent No. 6,490,620 to Ditmer et al. (hereinafter "Ditmer") and Zombek.

Claim 7 relates to a system that includes a first, monitoring computer, running a first program that monitors a network condition, a second, monitored computer, running a second program which allows said first program to monitor the network condition, and a connection between said first and second computers. The connection includes a firewall which blocks at least a first kind of non-HTTP communications but does not block HTTP communications. At least one of the first and second computers runs a third program that encapsulates network information indicative of the network condition into HTTP protocol.

The rejection asserts that Zombek describes encapsulating SNMP discovery information into an HTTP protocol.

As discussed above, the mere provision of standard SNMP services by SNMP console 130 neither describes nor suggests the HTTP encapsulation of SNMP messages, even when those messages are provided to a HTTP Server. Conventional SNMP communication thus appears to be available to SNMP console 130, whether

communicating with HTTP Proxy Back End Server 132 or with another of Zombek's servers. There is simply no indication that the API's provided by server SDK encapsulate registrations with SNMP console 130 into an HTTP protocol.

Nowhere does Zombek describe or suggest at least one of a first and a second computer that runs a third program that encapsulates network information indicative of the network condition into HTTP protocol, as recited in claim 7.

Ditmer adds nothing to remedy this deficiency in Zombek. As discussed in the response filed June 10, 2005, Ditmer describes a proxy interface and network computers that support SNMP functionality. *See generally Ditmer*, column 13, line 29-35; column 14 lines 20-26. However, Ditmer neither describes nor suggests that the information from SNMP, or in the words of claim 7 "network information indicative of the network connection" is encapsulated into HTTP, as claimed.

Since elements and/or limitations of claim 7 are neither described nor suggested by the cited art, a *prima facie* case of obviousness has not been established. Accordingly, applicant requests that claim 7, and the claims dependent therefrom, be allowed.

Independent Claim 12

Claim 12 was rejected under 35 U.S.C. § 103(a) as obvious over U.S. Patent No. 6,008,805 to Land et al. (hereinafter "Land") and Zombek.

Claim 12 relates to a method that includes forming an SNMP request for information from a remote computer, in a management station computer, changing said SNMP request to a form which will be passed by a firewall, wherein said changed SNMP request is encapsulated into HTTP protocol, and sending said changed SNMP request to said remote computer through said firewall.

The rejection asserts that Zombek describes encapsulating SNMP discovery information into an HTTP protocol.

As discussed above, the mere provision of standard SNMP services by SNMP console 130 neither describes nor suggests the HTTP encapsulation of SNMP messages, even when those messages are provided to a HTTP Server. Conventional SNMP communication thus appears to be available to SNMP console 130, whether communicating with HTTP Proxy Back End Server 132 or with another of Zombek's servers. There is simply no indication that the API's provided by server SDK encapsulate registrations with SNMP console 130 into an HTTP protocol.

Nowhere does Zombek describe or suggest changing an SNMP request to a form which will be passed by a firewall, wherein

said changed SNMP request is encapsulated into HTTP protocol, as recited in claim 12.

Land adds nothing to remedy this deficiency in Zombek. Land's device supports multiple management interfaces. However, Land neither describes nor suggests changing an SNMP request so that it is encapsulated into HTTP protocol, as recited in claim 12.

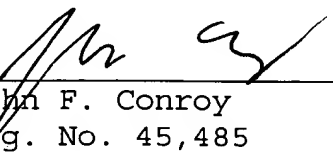
Since elements and/or limitations of claim 12 are neither described nor suggested by the cited art, a *prima facie* case of obviousness has not been established. Accordingly, applicant requests that claim 12, and the claims dependent therefrom, be allowed.

It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Applicant asks that all claims be allowed. No fees are believed due at this time. Please apply any charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: December 2, 2005



John F. Conroy
Reg. No. 45,485

Fish & Richardson P.C.
12390 El Camino Real
San Diego, California 92130
(858) 678-5070 telephone
(858) 678-5099 facsimile

10575351.doc
JFC/jhg